UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/617,913	07/17/2000	Richard W. Reece	11382.100A	8353

7590 08/05/2003

PATTON BOGGS LLP
2550 M Street, N.W.
Washington, DC 20037

EXAMINER
SEAL, JAMES

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 08/05/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/617,913	Applicant(s) REECE, RICHARD W.
	Examiner James Seal	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 17 July 2000

2. IDS dated 14 December 2000 and 26 June 2003 have been considered and a signed copy are enclosed.

3. Claims 1-5 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunstadt US 5003598 A, and further in view of Rabin, Transaction Protection by Beacons 1983.

5. As per claim 1, the limitation of an encryption station and a decryption section for encrypting plaintext into ciphertext is taught by Kunstadt (see Column 1, lines 35-40, Column 2, lines 37-38). The limitation of extracting keying material use for encryption and decryption of messages from a unrelated publicly available broadcast station being readily and reliably available at both sending (encryption station) and receiving (decryption station) locations is taught (Abstract, Column 1, lines 43-45, Column 2, lines 5-8). The limitation of selecting a portion of the public available broadcast station based upon *predetermined secret information* (applicant's private key) is disclosed by Kunstadt in the Abstract. Kunstadt is silent on using the unrelated publicly available broadcast station to transmit random number (Kunstadt method teaches the use of an

unrelated publicly available broadcast station to provide key material for an encryption and decryption station.)

6. Michael O. Rabin (Transaction Protection by Beacons) discloses the use of a beacon transmitting a sequence of randomly generated integers equally spaced in time from a satellite or a node in a network in which is equally accessible all participants, for the purpose of digitally signing contracts using a public key system when the two parties are remotely separated (Abstract and fifth paragraph page 237, and paragraph 1-4 page 258). One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teaching of Kunstadt and Rabin because creating keying materials from random numbers guarantees that the key will be random and hence the encryption most secure. Claim 1 is rejected.

7. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunstadt and Rabin as applied to claim 1 above, and further in view of Maurer US 5161244 A.

8. As per claim 2, the limitation of generating a synchronization signal (generating a time reference signal see Column 1, line 67, Column 2, lines 16-19) is disclosed by Kunstadt using, for example, WWV (time station, see Column 1, line 52-53). The limitation of selecting a portion of the public available broadcast station based upon *predetermined secret information* (applicant's private key) is disclosed by Kunstadt in the Abstract. As per the limitation of generating a sample block of bits based on time t see Rabin page 258-259 section 3, (The Beacon) and in particular 260 comment 1. the

limitation of accumulation random bits and storing them in memory (random number bit reservoir) is not taught by either Kunstadt or Rabin.

9. Maurer teaches the storage of random string strings in memory for later use at both sites (see figure 1, Column 8, lines 19-20, Column 12 lines 50-52). One of ordinary skill in the art would have been motivated to modify the Kunstadt/Rabin teaching without storage with Maurer's teaching of a with storage (random number reservoir) because it would alleviate the demand on the Kunstadt/Rabin system during peak usage and would provide extra security because the random number strings are now delayed (that is, it decreases the likelihood that an attacker simply recording the bits and correlates them against messages as the required storage needed by the attacker would then increase). Further such a modification encryption is perfect as long as the key (consisting of random bits) is as long as the message to be encrypted. Thus for long messages one would have to provide storage to accumulate necessary bits for encryption. Claim 2 is rejected.

10. As per claim 3, the limitation of determining the number of random bits that have been accumulated in memory, and comparing this number with a predetermined full value and if the number is less than the *predetermined* (full value) accumulate and store more bits. Consider figure 1 in Maurer. It is apparent from the figure that the random number generator RAN may be used either to directly encrypt the message the message or to accumulate random bits for the storage means STA (see doted line). The examiner asserts that storage devices must have finite capacity and thus must contain some feedback mechanism to which compares the amount of memory used to

the value when filled or some predetermined value, and to stop the accumulation process at that point. Failure to do so, would result is a waste of computer resources, both memory and computational. Claim 3 is rejected.

As per claim 4, the limitation of generating a new private key (new *predetermined secret information*) is disclosed by the Kunstadt/Rabin/Maurer combination. Maurer discloses the use of threshold storage (see Figure 1) as one means for global encryption (as opposed to direct encrypting). Maurer's RAN in the Kunstadt/Rabin/Maurer combination, would be replaced by Rabin's random number beacon using Kunstadt's predetermined secret information to refill the storage reservoir when the indicator went below some predetermine value. Again one of ordinary skill in the art would have been motivated to motify the Kunstadt/Rabin teaching without storage with Maurer's teaching of a refillable random number reservoir because it would alleviate the demand on the Kunstadt/Rabin system during peak usage and would provide extra security because the random number strings are now delayed. Claim 4 is rejected.

11. As per claim 5, the limitation that the station used for dispersing random number (beacon) be a satellite is disclosed by Rabin (page 257, paragraph 4). Claim 5 is rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703 746 7239 for regular communications and 703 746 7240 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

James Seal

James Seal
Examiner
AU 2131
July 29, 2003